



# National Security Cyber Assistance Program

Cyber Incident Response Assistance Accreditation

10 December 2014

**CONFIDENCE IN CYBERSPACE** 



#### **Admin Remarks**



- Fire Exits
- Restrooms
- Break Area
- Handicapped restrooms
- Please do not go beyond the main desk in the lobby
- Smoking Areas
- Personal Electronics Allowed sorry, no Wifi



# NSCAP Program and Accreditations



Agenda			
TIME	TOPIC	SPEAKER	
12:00 – 12:15	Introduction/Program Overview	Dawne Collura NSCAP Lead	
12:15 – 12:30	Partnering With Industry to Combat the Growing Cyber Threat	Jennifer Anderson Deputy Director IA OPS	
1:15 – 1:30	NSCAP History	Marie Dering NSCAP Co Lead	
1:30 - 1:45	Break		
1:45 – 2:45	CIRA Program Manual, Application Process, and Lessons Learned	Dawne Collura NSCAP Lead	
2:45 – 3:00	Break		
3:00 – 3:30	Future NSCAP Activities/Recap	Dawne Collura NSCAP Lead	
3:30 – 4:00	Questions/Closing Remarks	Dawne Collura NSCAP Lead	



### **Program Overview**



# Dawne Collura NSCAP Lead



### **Program Overview**



 The growing sophistication and number of cyber attacks necessitates an equally vigorous and rapid response.

 In exploring available approaches, the NSA/IAD developed a strategy to leverage the cyber expertise of industry and to supplement government cybersecurity manpower and resources.



### **Program Overview cont.**



 This strategic initiative is called the National Security Cyber Assistance Program or NSCAP.

 The purpose of NSCAP is to develop a list of accredited companies from which the National Security Systems (NSS) community can identify specific cybersecurity service providers.



# Partnering With Industry to Combat the Growing Cyber Threat



Jennifer Anderson
Deputy Director
IA OPS



# **Expanding Victim Set**



2009 - Present

Intellectual Property-rich targets & software firms

2005 - 2009



2000 - 2004



1990s





# Partnering With Industry to Combat the Growing Cyber Threat

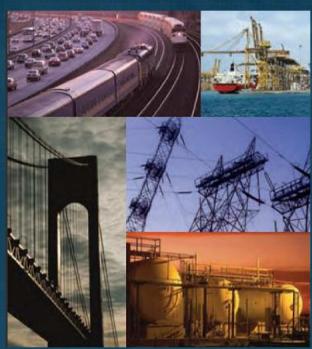


#### How We Engage: Direct Requests for Technical Assistance

- IAD provides awareness, evaluation, technical support
- Partners with DHS, DOJ/FBI, Treasury and others

#### Where We Engage:

- National Security Information Systems
- Defense Industrial Base Sector
- Energy Sector
- State/Local/Tribal Sector
- Critical Infrastructure Outreach
- And many others....





# Partnering With Industry to Combat the Growing Cyber Threat



 Increased Demand - for cyber response services is stretching government response capacity.



- Sophistication of cyber attacks require an equally vigorous and rapid response.
- **Join forces** with industry experts to *outmaneuver cyber adversaries*.
- Expand capacity, effectiveness and reach by building consensus.



### **Cyber Defense Landscape**



Confidence in Cyberspace video:

https://www.nsa.gov/public\_info/media\_center/ia/index.shtml





Marie Dering
NSCAP Co Lead





- Team and process building began in 2012
- Collection of government and industry best processes and procedures (2013)
  - Creation, review and acceptance of Intrusion
     Detection and Incident Response criteria
  - Cyber Incident Response Assistance (CIRA)
     Instruction Manual







**NIST SP800-53 -** Identifies 17 Families of Incident Assurance/Cyber Security controls.



CNSSI 1253 – Based on NIST SP800-53 controls, provides enhancements for NSS (includes enhancements in the 1253K Overlay\*.)



Both NIST SP 800-53 and CNSSI 1253 include the Incident Response Assistance (IR-7)

CNSSI 1010 – Focuses on organizations implementing 1 NIST control Family – Incident Response

Computer Security
Incident Handling Guide

Recommendations of the National Institute
of Standards and Technology

Paul Cichonski
Tom Mair
Tim Grance
Karen Scarfone

NIST SP800-61 Focuses on organizations or system owners implementing Incident Response controls





#### CIRA Pilot

- ARC announcement May 2013
- Industry Day 30 September 2013
- Receipt of packages began 10 October 2013
- Seven Companies Accredited 30 December 2013

#### First Formal CIRA Call

- ARC announcement 28 July 2014
- Receipt of packages began 6 August 2014
- Three Companies Accredited 30 September 2014



# **CIRA Accredited Companies**



#### **Company**

Booz Allen Hamilton, Inc.

Cincinnati Bell Technology Solutions Incorporated (CBTS)

CrowdStrike Services, Inc.

**Dell SecureWorks** 

FireEye, Inc.

Lockheed Martin Information Systems & Global Solutions

Maddrix, LLC

Mandiant, a FireEye Company

RSA Security LLC

Verizon



### **Legal Constraints**





- NSCAP does not charge for accreditations
- NSCAP does not pay companies to be accredited
- Submitting an application package does not guarantee accreditation
- Application packages are handled as PROPIN
- Accreditation does not result in a US Government security clearance
- Accreditation does not serve as a qualification for rendering services



### Legal Constraints, cont.





- Accreditation does not guarantee business or contracts with any NSS Owner/Operator or other customer
- NSCAP does not assist in any contracts or negotiations between a customer and an accredited company
- Participation in the accreditation process constitutes acceptance of these conditions
- NSCAP can ask for voluntary feedback of customer contacts and intrusion information



# Committee on National Security Systems Instruction



- Intent: CNSS National Manager will publish an instruction mandating the use of NSCAPaccredited companies by NSS Owners and Operators.
  - CNSS instruction initially drafted in 2013, currently revising in 2014
  - Review and approval by CNSS National
     Manager expected in 2015



## **CNSS Membership**



# The Committee is composed of a voting member from each of the following:

Secretary of State	Secretary of Defense	Secretary of the Treasury
Secretary of Commerce	Secretary of Transportation	Secretary Homeland Security
Secretary of Energy	Director, National Intelligence	Director, FBI
Director, CIA	Director, DIA	Director, NSA
Director, OMB	Assistant to the President for National Security Affairs	The Attorney General
Administrator, GSA	Chairman, JCS	COS, US Army
COS, USAF	Commandant, USMC	Chief of Naval Operations





### of NSCAP Accreditation



- NSA/IAD's accreditation is a nationally recognized validation of the quality of Cyber Incident Response Assistance (CIRA) services expected from and provided by accredited companies
- Accredited companies will be on the exclusive list of IADevaluated providers
- Accredited companies are pre-screened resources for the NSS or any community in need of specific cyber security services
- Companies, agencies or organizations can evaluate themselves against the NSCAP criteria as a performance benchmark for in-house CIRA activities and services





# **BREAK**

1:30 - 1:45



## **Application Process**



Dawne Collura
NSCAP Lead





# National Security Cyber Assistance Program

# CIRA Accreditation Process Overview

10 December 2014

CONFIDENCE IN CYBERSPACE



#### **NSCAP Accreditation**



 Accreditation is granted to companies that substantiate their expertise, processes and procedures according to the NSA/IAD methodology and industry standards via a comprehensive application package that contains supporting data.



### **Accreditation Overview**



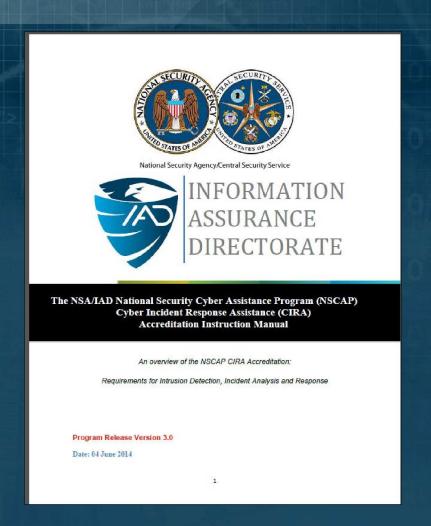
- Comprehensive application packages are submitted that contain defined processes and procedures, as well as supporting data and past performance
  - All submitted packages are handled as Proprietary Information (PROPIN)
- Accreditation is granted to companies that substantiate their expertise aligned to the NSA/IAD criteria as defined in the instruction manual
- This criteria was based on NSA/IAD methodology and industry standards and best practices
- NSA/IAD formal accreditation is valid for 24 months



# CIRA Accreditation Instruction Manual Version 3.0



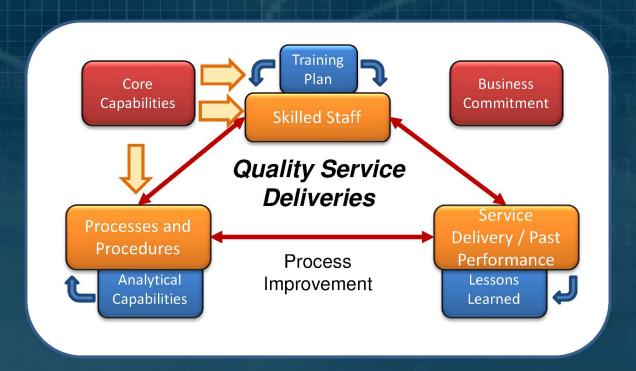
- The most current CIRA
   Accreditation Instruction
   Manual is Version 3 dated
   04 June 2014.
  - Accreditation under V2 extends to V3.
  - Changes are limited to Lessons Learned & Renewal Information.
- "go NSCAP NSA" on Internet





### CIRA Accreditation Instruction Manual





People
Processes
Performance



#### **Focus Areas Overview**



- Business Statement of Intent A formal, signed statement of commitment to the Cyber Incident Response (CIR) market
- Core Capabilities Overview An overview of the CIR services offered by the candidate company, to include marketing materials
- Processes and Procedures Formal documentation used when performing CIR Intrusion Detection & Analytical Services
  - Tell us HOW, not just WHAT
  - Analytical Capabilities Documentation that describes the facilities/tools used to perform data analysis



#### **Focus Areas Overview**



- Key Team Qualifications Profile sheets that identify education, training and/or credentials held by key employees (Appendix B)
  - Do not include Personally Identifiable Information (PII)
  - <u>Staff Personnel</u> should include the following:
    - CIR Team Leader, Incident Responder, CND Analyst (Forensics), CND Analyst and Auditor.
    - · Team must be available to support engagements when needed.
- <u>Training Plan</u> Documentation that describes how the company maintains the skills of technical and management staff



# Focus Areas Overview: Staffing Explanation



#### Skilled Incident Responders are required.

- Detailed processes and procedures require "competent" staff for consistent performance delivering focused services.
  - Generally scalable requires competent staff to scale
  - Limited in flexibility documentation cannot cover all possibilities.



### **Focus Areas Overview**



- 3 Past Performance Reports (within the last 24 months)
  - Content should be redacted
  - Successful past performance helps identify capabilities and effectiveness of processes and procedures
  - <u>Lessons Learned</u> validates effective processes and procedures and provides for corrective actions/process improvements for those that aren't.
- Client Furnished Information and Data Management –
   Capabilities to manage property and information securely
  - Receipt of government/customer furnished data, information or material
  - Establishes a capability for the candidate company's receipt of Government provided classified information
  - Chain of custody of material and data





# **Application Package Assembly**



### **Application Package Assembly**



- All submitted sections should address the focus areas described in the Instruction Manual, Section 6, Accreditation Application Package Contents.
  - The section content is mandatory and it is highly recommended to follow the format.
  - 2. Completing the Applicant Content Checklist, in Appendix C, ensures that the application package is complete.
  - 3. Application packages will not be accepted for evaluation if they are incomplete.



# Appendix A Process & Procedure Guide



- All submitted sections should address the capabilities described in Appendix A
- Each capability section within Appendix A includes an example, titled "Potential Documentation Content" [Modeled after NIST SP800-53A (i.e., Potential Assessment Methods and Objects).]
  - The example is provided as an approach for use within a Process or Procedure.
  - 2. It is highly recommended to follow the format.



#### **Focus Areas**



#### **FOCUS AREAS**

- Business Statement of Intent
- Core Capabilities
- Process & Procedures (Overview)
- CIRA Key Team Qualifications Report
- CIRA Education & Training
- Past Performance
- Client Furnished Information & Data



# Process and Procedures Focus Area Capabilities



## PREPARATION & PLANNING

- Services Agreement
- Client Engagement Management
- Communication Management
- Preliminary Data
   Collection
- Engagement Tools & Resources
- Travel Management
- Rules of Engagement

## INCIDENT IDENTIFICATION, DETECTION & ANALYSIS

- Log Collection & Analysis
- Network Traffic Data Collection & Analysis
- Host Integrity Data
   Collection & Analysis
- Incident Analysis

# CONTAINMENT & REMEDIATION RECOMMENDATIONS

- Incident Containment Remediation
- Post-Incident Analysis & Final Report
- Lessons Learned





# CIRA Team Qualifications Guide Appendix B





- It is critically important that personnel providing CIR services to NSS owners have sufficient skills to perform the work identified in their employers' processes and procedures.
- The Candidate Company's CIR Team is expected to:
  - meet the Capabilities of the candidate organization's business model
  - meet the demands of their CIR clients
  - deliver the CIR services the candidate organization has documented in its internal policies and procedures
  - be eligible for a security clearance





- The following applies to the staff assessment process:
  - The NSA/IAD will not directly assess or interview candidate company's CIR Team members.
  - The candidate company is required to present the skills of five different
     Key Team Members as part of the Accreditation Application.
- Each Key Team Member must have specialized expertise
  - Expertise is identified through their possession of a combination of skills/certifications/education and/or experience.
  - Certifications alone will not meet the capabilities of this accreditation.
  - The certifications identified are either recognized by the DOD or by members of the Incident Response community. DOD recognition is substantiated in DOD Manual 8570.01- updated 03/29/2013.
  - See Table 3 and Table 4 for certification and accreditation lists and information.





 The primary job functions of the five (5) required individuals are identified in the Application Manual, Table 2: CIRA Key Team Qualifications Guidance

Key Team Member Specialization
CIRA Team Leader
Incident Responder
CND Analyst (Forensics)
CND Analyst
Auditor / Vulnerability Analyst

- Only one full-time individual is allowed per key team member position;
   the positions cannot be shared responsibilities between team members.
- All 5 key individuals must be available to deploy on each engagement





- Additional technical (MCSE, CCIE, etc.) or administrative personnel (PMP, etc.) may be assigned to the CIR Team but those individuals do not count towards meeting the accreditation capabilities.
  - For companies: Part time contractors, subcontractors and other resources may be part of the organization's CIR Team but any individual certifications from those other organizations *may not be* counted toward this accreditation.



## **Application Submissions**



- In addition to the completed capabilities sections, submit the forms included in Appendix C with your application package
  - Add supplemental documentation as needed, i.e., support team credentials excluding PII
  - Each submitted section should be marked separately with your company's name and the name of the capability section.



## **Application Content Checklist**



- The application checklist must be completed by the applicant and submitted with the application.
- The last column will be completed by the NSCAP evaluation team.

#### 4 Application Content Checklist for a Candidate Organization

Document Name	Description					
		Document Name	Description	Included in the Package? (Y/N)	Applicants' Document Name	NSA/IAD Verified
Business Statement of Intent	A formal statement by the candidate organization asserting its commitment to perform CIRA services.  Documentation that descriptions are common to the common training that descriptions are carried to the carried to t	CIRA Team Qualification Documentation	Documentation that describes how the candidate organization employs skilled and capable individuals to deliver CIRA services to its clients.			
Overview	the core capabilities that describe how a candidate organization performs CIRA analysis.	CIRA Education and Training	Evidence that the candidate organization's technical and management staff are keeping up to date on current CIRA techniques.			
Processes and Procedures	Processes and procedures used to perform and delive CIRA services.	Past Performance	At least three (3) final reports, modified to protect the client's identity, generated at the conclusion of separate CIRA Service engagements performed by the candidate organization in the previous 24 months.			
	Preparation and Plans     Services Agreement     Olient Engagement					
	Management Process o Communication Management Process o Preliminary Data Collection	Customer- Furnished Information and Data	Identifying the candidate organization's capabilities to manage customer property and information in a secure manner.			
	o Engagement Tools an Resources Identificati o Travel Management Processes	Document Identification	Are all Documents Labeled with corporation name and document title in the file name			
4/1/14	o Rules of Engagement	CoverLetter	Signed by authorized Individual?			



## **Application Package Scoring**



- A blank score sheet template will be posted to the NSCAP.nsa.gov web page
- This standard score sheet is used for each application
  - Each capability is assigned a weighted value
  - Each capability can achieve one of three scores:
    - 0% Non-Compliant
    - 70% Partially Compliant
    - 100% Compliant



## **Application Package Scoring**



- Passing score = 85 points
  - Points = sum of weighted values X scores awarded for each capability
- Impact of 0% and 70% scores
  - Low scores in highly weighted capabilities will have the most overall impact
  - Low scores even in less weighted capabilities can affect the final score



## **NSCAP Scoring**



Network Traffic Data Collection and Analysis (Technical Review)								Evaluator hours	Peer hours	Page count
(CIRA Accreditation Instruction Manual, Appendix A, Section 3.2)				Yes	Suff.	. No	Comments			
Does the Candidate's Application Package contain processes/procedures marked as "Network Traffic Data Collection and Analysis"?			(C)							
Capability Reminder: Does the process or proc to perform the work, 2. When c an the work be p 4. What tools or resources will be needed to per	erformed (d	lepender								
Capability 1: Does the Candidate have procedures to collect protocol derived network traffic?										
Capability Reminder 1: The intent of this activi crosses the client's external and internal bound network Virtual Local Area Networks (VLANs) perform this collection on the client's work site.	aries, as wel The Candida	ll as trafj ate Orga	îc betwe	en no	odes a	and systems on the				
3. Capability 2: Does the Candidate have procedures to analyze IPv4 and IPv6 network traffic?										
Capability Reminder 2: The intent of this activity traffic data as it crosses the client's external and systems on the network Virtual Local Area Netwability to perform this analysis on the client's wa	l internal bo orks (VLAN	oundarie	s, as wel	l as t	raffic	between nodes and				
4. Capability 3: Does the Candidate have procedures to engage the client's technical resources to obtain the required data?  (C)										
Capability Reminder 3: The intent of this activi made should client resources be required to col- contained in the Communication Plan or in othe the assessment team providing them with guidar	lect or trans <sub>i</sub> er document	port log. ation an	s for ana ad should	lytice l pro	al pur vide s	rposes. This may be pecific instructions to	,			
6. Capability 4: Does the Candidate have procedures to assess the system risk posture based on the network traffic analysis and report those findings to the client?										
Capability Reminder 4: The Candidate Organization must include processes to assess the system risk posture based on the Network Traffic analysis and report those findings to the client. Network Traffic analysis may result in identifying significant, new or escalating risks to the affected system or systems. The processes and procedures should clearly identify the approaches that the assessors would normally take to report those identified or potential changes in the system's overall risk posture. This would include identifying the threat or exploit, what is affected, and when it occurred.										
CIRA Priority	14pt	ts		Not	es:		•		•	•
Network Traffic Data Collection and Analys	sis Scor	re Value	Select							
				-						
Non-Compliant	70	% 9.5 % 9.5		-						
Partially-Compliant Compliant	100		_	1						
Соприин	100	70 1-								



# Accreditation Decisions and Reaccreditations



- Accreditation letters are signed by the IAD Director
- Non-accreditation letters include application feedback from the NSCAP Program Manager
- Main Factors in Non-Accreditation Decisions
  - 1. Didn't follow the Instruction Manual
  - 2. Received team bios instead of their expertise/training for their key team role
  - 2. Included too much WHAT and not enough HOW
  - 3. Lack of proof of defined, repeatable processes and procedures
- Reaccreditation reminders are sent 30 days before expiration, with a 30 day evaluation window





## BREAK

2:45 - 3:00





## **Future NSCAP Activities**

**CONFIDENCE IN CYBERSPACE** 



## **2015 Application Submissions**



- In CY2015, applications will be submitted and evaluated via the NSCAP Accreditation Portal (NAP)
  - NAP Phase 1 (new applications) is in the final development and testing stage
  - NAP Phase 2 will address accreditation renewal applications
  - Uploaded attachments should not exceed 5MB in size



### **NSCAP Accreditation Portal**



# National Security Cyber Assistance Program

Welcome quest

#### General Information

Home Contact Us Security Warnings Login/Join

#### Downloads

Accredited Organizations Accreditation Instruction Manual Applicant User's Guide Welcome to the National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA) Accreditation Portal

The NSA/IAD National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA) accreditation was designed to meet the growing needs of the U.S. Government, supplementing the incident response and intrusion detection services that NSA/IAD provides to the DOD, IC, and other organizations as authorized and directed. The core objective of CIRA accreditation is to identify companies qualified to provide rapid, on-site support to National Security Systems (NSS) owners and operators in incident response and intrusion detection. Broadly speaking, assessment of capabilities is based on the ability to:

- Consistently deliver services using repeatable processes and procedures.
- Assign highly skilled and qualified staff, who are eligible to hold U.S. Government Security clearances, to follow outlined
  processes and procedures to deliver services.
- Maintain and improve the quality of delivered services through training initiatives, improvement of analytical capabilities, and
  use of lessons learned from previous deployments or engagements to refine processes.

CIRA accreditation is awarded to qualified CIRA providers who are capable of providing comprehensive CIRA services to operators of classified and unclassified National Security Systems (NSS).

Within this site, guidance is provided on how to log-in, how your application will be processed and a time line that you can expect between the submittal of your application and our completion of its review. Have questions or want to provide feedback? Click Contact Us.

What's New?

There are no current notices posted.

Privacy | Terms of Use | NSA.gov | NoFEAR Act | FOIA | IAD.gov





## **Future NSCAP Activities**



- Next call for CIRA Application Packages
  - First quarter of CY2015
  - Announcement will be posted on the Acquisition Resource Center (ARC) website, forwarded via ARC email and posted on the NSCAP@nsa.gov web site.
- Government Industry Day
  - Second quarter of CY2015
- Next Industry Forum Day
  - TBD



## **NSCAP Information Resources**



- Internet URL: https://www.nsa.gov/ia/programs/ cyber\_assistance\_program/
- Google: NSCAP NSA
- ARC website
- Internet Email: NSCAP@nsa.gov





## https://www.nsa.gov/ia/programs/cyber\_assistance\_program/

Information Assurance

About IA at NSA

IA Client and Partner Support

IA Nevs

IA Events

IA Mitigation Guidance

IA Academic Outreach

IA Business and Research

\* IA Programs

Commercial Solutions for Classified Program

Global Information Grid

High Assurance Platform

Inline Media Encryptor

Suite B Cryptography

NSA Mobility Program

National Security Cyber Assistance Program

IA Careers

Contact Information

Home > Information Assurance > Programs > Cyber Assistance Program

SEARCH

#### National Security Cyber Assistance Program

#### Processes, People, Performance

The growing sophistication and number of cyber attacks necessitate an equally vigorous and rapid response. In exploring viable approaches to more vigorously defend against cyber threats, NSA developed a strategy to leverage the cyber expertise of industry. This newly formed strategic initiative is called the **National Security Cyber Assistance Program**, or **NSCAP**.

#### What's New

- Call for Applications (Closed)
- NSCAP CIRA-Accredited Companies'
   Contact Information
- IAD Announces First Accredited Companies in NSCAP

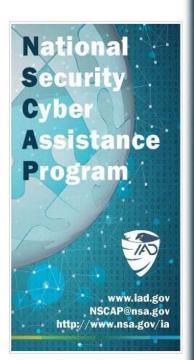
#### **Program Information**

- How NSCAP Benefits Service Providers and NSS Owners
- NSCAP Overview (Printable Brochure)
- FAQs
- Critical Focus Areas
- Journal of Information Warfare Article (p. 49 of 111)

#### **Program Documentation**

CIRA Instruction Manual V3

Questions? Feedback? Contact the NSCAP
Office: NSCAP@nsa.gov



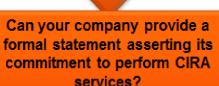


# Does Your Company Have What It Takes?



## DOES YOUR COMPANY HAVE WHAT IT TAKES TO GET ACCREDITED?

Can your company deploy a team onsite to support an NSS owner/operator to deliver incident response and/or intrusion detection services?



Can your company provide overview documentation describing the baseline processes used to conduct CIRA services, tactics and techniques?

Are your key CIRA personnel capable of receiving or eligible to receive a US Government security clearance?

Does your company have a deployment team of 5 full-time key personnel, at a minimum, whose primary job function is the support or delivery of CIRA services?

Does your company utilize documented, detailed processes and procedures (TTPs) that are repeatable per incident?

Does your company have a documented plan for key CIRA personnel to take ongoing education and training to address emerging technologies and threats?

Can your company submit documentation to show past performance of at least 3 incident response engagements within the last 24 months?

Can your company submit detailed processes and procedures used to manage customer property/information obtained during a CIRA engagement?





# Questions?

Email: NSCAP@NSA.gov







## BACK UP SLIDES



# Appendix A Processes & Procedures



- Section 1.0 Preparation and Planning
  1.1 Elements of a CIR Services Agreement
- Capability: Utilize processes and procedures that, when followed, would be expected to develop a mutually acceptable CIR Services Agreement.
  - Ad hoc engagement processes may overlook important details.

### Of interest:

 Documentation that establishes technical objectives that are sought to be included in an agreement.





Section 1.0 Preparation and Planning (cont.)

- 1.2 Client Engagement Management
- Capability: ... that identify their approach to engage the client to fulfill the CIR Services Agreement.
  - Successful client engagement processes balance roles and responsibilities of Sales, Contracts and Technical interests.
- Of interest:
  - Boundary responsibility documentation
  - Process flow documentation that support client engagements.





Section 1.0 Preparation and Planning (cont.)

- 1.3 Communication Management
- Capability: ... that facilitate initial and on-going communications between the CIR Team and the client.
  - Teams include multiple people with different roles and responsibilities.
  - Teams are usually supported by multiple client contacts (e.g. SAs, DBAs, NW Engineers, etc.)
  - Data collection and incident response priorities can conflict.

#### Of interest:

 Processes that address prioritizing and coordinating support requests within the CIR team.





Section 1.0 Preparation and Planning (cont.)

- 1.4 Preliminary Data Collection
- Capability: ... request that the client collect incident-related information that could be used to facilitate the engagement efficiency prior to the arrival of the CIR Team.
  - Collecting data prior to the teams arrival could accelerate response.
- Of interest:
  - Standard, structured requests for the collection of incident data can expedite performance and increase efficiency
  - Cross references to other processes and procedures (e.g., Agreement Objective content, etc.) could be beneficial





### Section 1.0 Preparation and Planning (cont.)

- 1.5 Engagement Tools and Resources
- Capability 1: ... that the CIR Team exercises appropriate engagementspecific planning prior to initiating work on the client's systems or system environment.
  - Planning may be based on:
    - Capabilities within the negotiated agreement
    - Incident Characteristics collected and received through Preliminary Data collection
    - Needed CIR Team Staff skills,
    - Needed tools patches and updates, and identifiers (signatures, characteristics, etc.)
    - Needed collected data protection Capabilities
    - Needed Event Correlation and other analytical tools needed to perform the work scope.
    - Other engagement needs identified by work scope/Provider's Business Service model

#### Of interest:

 Processes that identify advanced detailed planning that the engagement team follows to avoid missed service agreement details. (See how this is stated in the Manual)





Section 1.0 Preparation and Planning (cont.)

- 1.5 Engagement Tools and Resources (cont.)
- Capability 2: When preliminary data is collected, ... include the performance of analysis on that collected data to determine engagement-specific needs.
  - Analysis should be performed on all collected data received.
  - Results should be used to support Capabilities planning.

### Of interest:

- Processes that identify the provider's standard approaches to analyzing any preliminary data that was collected and provided.
  - · May be differentiated between off site and on-site data analysis as appropriate
  - Should include processes that identify data protection methods as appropriate
- Processes that use the outcomes from the analysis as part of the planning process.





Section 1.0 Preparation and Planning (cont.)

- 1.6 Travel Management
- Capability: ... that facilitate the CIR Team's rapid deployment to destinations identified within the CIR Services Agreement.
  - Rapid, efficient and timely deployments are the goal.
- Of interest:
  - Processes that facilitate travel while avoiding delays.





Section 1.0 Preparation and Planning (cont.)

### 1.7 Rules of Engagement

- Capability: ... that the CIR Team is briefed and is fully cognizant of the candidate organization's normal engagement process and of any specific engagement restrictions or capabilities required prior to beginning work on the clients' site or accessing the clients' systems.
  - Each Client engagement, agreement and scope is different.
  - As individuals and teams become more experienced, there is a potential for individuals losing sight of each agreement's expectations, deliverables, schedules and constraints.

#### Of interest:

- Processes for preparing a program Kick off briefing.
- Processes for ensuring that program kick off is held and identifying what those meetings cover.





- 2.1 Log Collection and Analysis How does your company:
  - Collect logs,
  - Perform log aggregation and
  - Transition to Incident Analysis?
- 2.2 Network Traffic Data Collection and Analysis How does your company:
  - Collect Network Traffic data,
  - Perform aggregation and
  - Transition to Incident Analysis?
- 2.3 Host Integrity Data Collection and Analysis How does your company:
  - Perform Host Integrity checking on different platforms, perform aggregation and transition to Incident Analysis?
- 2.4 Incident Analysis How does your company:
  - Aggregate diverse data sets,
  - Ingest data into an automated systems,
  - Perform analysis,
  - Verify and Report Results?





- 3.0 Containment and Remediation Recommendations How does your company:
  - Prepare, Review and offer Recommendations for Containment and Remediation,
  - Perform Source Attribution,
  - Perform Damage Assessments, and
  - Generate Incident Metrics?
- 4.0 Post Incident Analysis How does your company:
  - Prepare, review and present a summary of the Engagement to the client?
- 5.0 Lessons Learned How does your company:
  - Conduct an internal lessons learned at the conclusion of each engagement, and
  - Use the results of the lessons learned exercise to improve processes?



# Focus Areas Overview: Staffing Explanation



- The company's business model dictates its approach.
  - It selects a model that optimally meets its needs.
- No one approach is better than another. Striking a balance will be considered in the evaluation process.
  - Approach effectiveness is partially validated in:
    - Past performance reports and
    - Numbers of successful service engagements delivered.



## **Incident Response Methodology**



